Michael F. Ram (SBN 104805)
mram@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
T: (415) 846-3862
F: (415) 358-6923

John A. Yanchunis*
JYanchunis@forthepeople.com
Ronald Podolny*
ronald.podolny@forthepeople.com
Antonio Arzola*
arzola@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DOUGLAS CLEMMERSON, individually and on behalf of all similarly situated persons, Plaintiffs, v. AFFIRM HOLDINGS, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF**

Plaintiff Douglas Clemmerson ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Affirm Holdings, Inc. ("Affirm" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for failing to secure its systems and data from cyberattacks and for failing to conduct sufficient due diligence before entrusting the non-public PII of Defendant's customers to Evolve Bank & Trust ("Evolve"), a third-party bank with deficient data security measures.

2. Defendant Affirm is a financial technology software application ("fintech app"). The company offers an online platform which provides lending and consumer credit services, as well as enables customers to buy what they want and pay over time. Affirm serves customers in the United States.[1] It is headquartered at 650 California Street, San Francisco, CA 94108.

3. Affirm uses Evolve Bank & Trust ("Evolve") as its banking partner. Evolve is a bank that accepts deposits, makes loans, and provides mortgage solutions, card facilities, and online banking services. Evolve serves clients in the United States. Evolve works with fintech startups by providing banking services to these start-ups' clients. Affirm website states: "The Affirm Card is a Visa® debit card issued by Evolve Bank & Trust, Member FDIC, pursuant to a license from Visa U.S.A. Inc."[2]

4. On or about June 25, 2024, Evolve announced that a "known cybercriminal organization" stole its customers' personal identification information ("PII") and posted it on the dark web (the "Data Breach"). This PII included Affirm customers' data. The data which the Defendant collected from the Plaintiff and Class Members, and which was exfiltrated by

[1] Bloomberg, "Affirm Inc.", https://www.bloomberg.com/profile/company/1276532D:US?embedded-checkout=true

[2] Affirm, https://www.affirm.com/how-it-works/why-affirm (last accessed on July 31, 2024).

cybercriminals from the Defendant, were highly sensitive. Upon information and belief, the exfiltrated data included personal identifying information ("PII") like individuals' names, health insurance and treatment information.

5. Upon information and belief, prior to and through the date of the Data Breach, the Defendant obtained Plaintiff's and Class Members' PII and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, Affirm performed inadequate, if any, due diligence before selecting Evolve as its banking partner, including permitting it to store Affirm's clients' PII and other sensitive information.

6. Upon information and belief, the risk of the Data Breach was known to the Defendant. Thus, the Defendant was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

7. Then, after the Data Breach, the Defendant failed to provide timely notice to the affected Plaintiff and Class Members—thereby exacerbating their injuries. Ultimately, the Defendant deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, the Defendant impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

8. Even when the Defendant finally notified Plaintiff and Class Members of their PII's exfiltration, the Defendant failed to adequately describe the Data Breach and its effects.

9. Today, the identities of Plaintiff and Class Members are in jeopardy—all because of the Defendant's negligence. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial accounts.

10. Armed with the PII stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

11. Plaintiff and Class Members will likely suffer additional financial costs for

purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

13. Through this action, Plaintiff seeks to remedy these injuries on behalf of themselves and all similarly situated individuals whose PII were exfiltrated and compromised in the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

15. Plaintiff Clemmerson is a natural person and citizen of Parker County, Texas. Clemmerson is a customer of Defendant Affirm.

16. Defendant Affirm is a financial technology software application ("fintech app"). The company offers an online platform which provides lending and consumer credit services, as well as enables customers to buy what they want and pay over time. Affirm serves customers in the United States.[3] Affirm uses Evolve as its banking partner.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00, exclusive of interest and costs, and all conditions are met. In particular, Plaintiff is a resident of a

[3] Bloomberg, "Affirm Inc.", https://www.bloomberg.com/profile/company/1276532D:US?embedded-checkout=true

state different from Defendant Affirm.

18. This Court has jurisdiction over Defendant Affirm because Affirm conducts significant business in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District and Defendant Affirm is headquartered in this district.

GENERAL FACTUAL BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and Class Members

20. Defendant Affirm uses Evolve bank to effectuate payment as for similar purposes, as its official banking partner. Evolve is a bank. It accepts deposits, makes loans, and provides mortgage solutions, card facilities, and online banking services. Evolve serves clients in the United States.

21. As a condition of receiving Affirm's services, Defendant requires that its customers entrust Affirm with highly sensitive information, including their PII.

22. Upon information and belief, numerous fintech apps used Evolve as their banking partner. One of these entities was Affirm. Within this relationship, Affirm transferred and entrusted data, including Plaintiff's and Class Members PII, to Evolve.

23. Upon information and belief, Evolve received and maintained the PII of Affirm's customers, such as individuals' names, addresses, dates of birth, and Social Security numbers. On information and belief, these records are stored on Affirm's and Evolve's computer systems.

24. Because of the highly sensitive and personal nature of the information Defendant acquire and store, Defendant knew or reasonably should have known that it stored protected PII and must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' PII and provide adequate notice to customers if their PII is disclosed without proper authorization.

25. When Defendant collects this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

26. Defendant acquired, collected, and stored, and represented that it maintained

reasonable security over Plaintiff's and Class Members' PII.

27. Upon information and belief, Affirm made no, or insufficient, efforts to ensure that Evolve complied with the requisite data security standards, and all federal and state laws regarding PII protection, before entrusting its clients' data to Evolve.

28. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

29. Affirm represented that it took customer data security seriously and undertook to protect customer PII.

30. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

31. Upon information and belief, Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

32. Affirm could have prevented or mitigated the effects of the Data Breach by selecting a banking services provider that employs reasonable security measures to protect its customers' information.

33. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

34. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

35. Affirm failed to conduct the necessary inquiries into Evolve data security practices, and selected Evolve, which had inadequate information security practices, as its banking partner.

Affirm then provided its customers' PII to Evolve, despite this entity's inadequate information security practices.

36. Affirm failed to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed.

37. Defendant failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and potentially disclose it to others without consent.

38. Upon information and belief, Affirm failed to ensure that Evolve had implemented such processes before selecting Evolve as its services provider.

39. Upon information and belief, Affirm failed to ensure that Evolve employed encryption in a reasonable manner, or at all, before selecting Evolve as its banking services provider.

The Data Breach

40. On or about June 25, 2024, Evolve confirmed that it was the subject of a ransomware attack. The Data Breach was allegedly perpetrated by Lockbit ransomware gang. The bank confirmed that hackers "released illegally obtained data, including Personal Identification Information ("PII"), on the dark web."[4] "The data varies by individual but may include your name, Social Security Number, date of birth, account information and/or other personal information," the bank explained.[5]

41. A number of fintech startups were affected by the Evolve Data Breach. Industry publication TechCrunch reported that, among others, fintech startups Branch, EarnIn, Marqueta, Melio, Mercury, Yieldstreet and Wise were affected, and their customers' PII may have been stolen.[6]

---

[4] James Reddick, "Evolve Bank confirms data breach after brazen LockBit claims" (June 26, 2024), https://therecord.media/evolve-bank-data-breach-lockbit (last visited July 4, 2024).

[5] *Id.*

[6] Lorenzo Franceschi-Bicchierai, "Yieldstreet says some of its customers were affected by the Evolve Bank data breach" TechCrunch (July 2, 2024), online: https://techcrunch.com/2024/07/02/yieldstreet-says-some-of-its-customers-were-affected-by-the-

42. On its website, Evolve posted a statement, which acknowledges that Evolve was targeted in a ransomware attack, in which ransomware gang LockBit leaked its customers' PII. The statement reads, in part:

> **What Happened**
>
> In late May 2024, Evolve Bank & Trust identified that some of its systems were not working properly. While it initially appeared to be a hardware failure, we subsequently learned it was unauthorized activity. We engaged cybersecurity specialists to investigate and determined that unauthorized activity may have been the cause. We promptly initiated our incident response processes, stopped the attack within days, and have seen no new unauthorized activity since May 31, 2024. We engaged outside specialists to investigate what happened and what data was affected, as well as a firm to help us restore our services. We reported this incident to law enforcement.
>
> While the investigation is ongoing, we want to share some important information about what we know so far. At this time, current evidence shows the following:
>
> - ***This was a ransomware attack by the criminal organization, LockBit***.
> - They appear to have gained access to our systems when an employee inadvertently clicked on a malicious internet link.
> - There is no evidence that the criminals accessed any customer funds, but ***it appears they did access and download customer information from our databases and a file share during periods in February and May***.
> - The threat actor also encrypted some data within our environment. However, we have backups available and experienced limited data loss and impact on our operations.
> - We refused to pay the ransom demanded by the threat actor. ***As a result, they leaked the data they downloaded***. They also mistakenly attributed the source of the data to the Federal Reserve Bank. (Emphasis added.)

43. Jason Mikula, a fintech reporter, wrote on June 20, 2024, that "The situation at Evolve Bank & Trust, which powers dozens of fintech programs with millions of end users, went from bad to worse last week." While Evolve was "still struggling to deal with the fallout from the

---

evolve-bank-data-breach/ (last accessed July 2, 2024).

bankruptcy and reconciliation issues linked to one-time banking-as-a-service partner Synapse", the bank was hit with "what may be one of the widest-reaching public data breaches in US history." Mr. Mikula reported that the Data Breach involved the exfiltration of some 33 terabytes of data, equivalent to some 2.8 billion pages of text.[7]

44. Mr. Mikula noted that Evolve is "arguably the most prolific partner bank supporting fintech programs" and has "powered services or capabilities" for the following firms, all of which have likely lost their clients' PII in the Data Breach: Affirm, Airwallex, Alloy, Apto Payments, Asset Lab, B9, Bilt, BlockFi (bankrupt), Bond (BaaS platform acquired by FIS), Branch (powers instant payout and EWA programs for major business like Uber and Fetch and franchise operators of brands like Pizza Hut, Jimmy John's, and Dunkin Donuts), Brightside, Buffpay, Bushel Exchange, ByteFederal, Cadre, ChangeFi, Clearing, Dave, Deserve (credit card-as-a-service platform), Earnin', EquityZen, eusoh, Every, Extra, Finch Money, FloatMe, Flycoin, FTX (bankrupt), Gerald, Grid, GigWage, GloriFi (shutdown), GoChanged, GravyStack, Hightop, Juno, Kyshi, Lumanu, Melio, Mercury, Nomad, Paceline, Palolo, PayGears, Paystand, PrideCard, PrizePool, Profit Business Bank, Qoins, RBR, RelayFi, Rho, Rollfi, Sail, Save, Series Financial, Shopify (via Stripe Treasury), Sila (payment processing platform), Sila, Solid (banking-as-a-service platform), SoLo Funds, Starlight, Status Money (shutdown), Step, Stilt (acquired by JG Wentworth), Stripe Treasury, Swype, Synapse (ongoing bankruptcy), TabaPay, TeamUP, Unbanked, Wise (until late 2023), YieldStreet, Yorbis, ZELF, and Zirtue.[8]

45. Evolve's poor cybersecurity practices are long-standing and led to regulatory action against Evolve. The St. Louis Federal Reserve Bank and the Arkansas State Banking Department launched a "wide ranging enforcement action" against Evolve, stemming from their 2023 safety and soundness examination. The enforcement action mandated "a plan and timetable to correct

[7] Jason Mikula, "Evolve Hack Crisis: Russia-Linked cybergang Leaks Records on Millions" *Fintech Business Weekly* (June 30 ,2024), https://fintechbusinessweekly.substack.com/p/evolve-hack-crisis-russia-linked (last visited July 3, 2024).

[8] *Id.*

information technology security deficiencies."[9]

Actions Following the Data Breach

46. Following the Data Breach, the Plaintiff received a letter from Defendant Affirm, attached hereto as Exhibit "A", which stated, in relevant part:

> We are writing to inform you that some of your personal information was recently impacted when Evolve Bank & Trust ("Evolve") was the victim of a cybersecurity attack. Evolve provides financial services including Banking-as-a-Service products to host accounts and provide mobile banking. **This incident did not impact your funds stored with Evolve**.
>
> Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring.
>
> **What happened?**
>
> On May 29, 2024, Evolve identified that some of its systems were not working properly. While it initially appeared to be a hardware failure, we subsequently learned it was unauthorized activity. Evolve promptly initiated its incident response processes and stopped the attack. No new unauthorized activity on Evolve's systems has been identified since May 31, 2024. An investigation with assistance from a cybersecurity firm was initiated to investigate what happened and what data may have been impacted. Evolve also notified law enforcement and worked to add further protections to harden its systems.
>
> **What personal information was involved?**
>
> There is no evidence that the threat actors accessed any customer funds, but it appears the threat actors did access and download customer information from Evolve's databases and a file share during periods in February and May 2024.
>
> Within these downloaded files, Evolve identified the following personal information about you: Social Security Number.
>
> **What we are doing:**
>
> Evolve is offering you a complimentary 24-month membership to TransUnion's credit monitoring and identity theft protection services. We are also providing you with proactive fraud assistance to help with any questions that you might have or in the event

[9] Jason Mikula, "Evolve Hit with Fed Enforcement Action, But Why Did It Take This Long?" *Fintech Business Weekly* (June 23, 2024), https://fintechbusinessweekly.substack.com/p/evolve-hit-with-fed-enforcement-action (last visited July 3, 2024).

that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Please see Attachment A below for additional details regarding these services. **You must enroll by October 31, 2024, to receive these services**.

Prior to the incident, Evolve had a significant number of cybersecurity measures in place. Since becoming aware of the incident, Evolve has taken steps to further strengthen its security response protocols, policies and procedures, and its ability to detect and respond to suspected incidents.

What you can do:

It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. You can also enroll in the TransUnion service being offered to you. Additional information about how to protect your identity and personal information is contained in Attachment B below.

For more information:

A dedicated call center is also being set up to answer your questions about this incident. You may call it toll free at 866-238-9974, Monday through Friday 8 a.m. to 8 p.m. ET (excluding major U.S. holidays).

47. In sum, aside from offering a 24-month credit monitoring and identity theft protection services, which is wholly inadequate, because the risks of identity theft continue for a lifetime, the Defendant largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

48. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[10]

49. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey,

[10] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed March 18, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, *https://www.bls.gov/news.release/pdf/wkyeng.pdf* (last accessed March 18, 2024) (finding that on average, private-sector workers make $1,145 per 40-hour work week.).

American adults have only 36 to 40 hours of "leisure time" outside of work per week;[11] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[12] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

50. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

51. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

52. Aside from the offer of 24 months of identity monitoring services, which is inadequate for reasons described above, Defendant has offered no measures to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for their respective lifetimes.

53. Affirm had and continues to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

54. Plaintiff and the Class Members remain, even today, in the dark regarding the scope of the data breach, what particular data was stolen, beyond several categories listed in the letter as "included" in the Data Breach, the particular ransomware used, and what steps are being taken, if

[11] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019) (last accessed March 18, 2024).

[12] *Id.*

any, to secure their PII and financial information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly the Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

55. Plaintiff's and Class Members' PII and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and financial information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

RANSOMWARE THREATENS FINANCIAL SERVICES

56. Ransomware is a subset of malware in which the data on a victim's computer, or network, is locked, typically by encryption, and where payment is demanded as a condition of providing the decryption key to unlock the encrypted data and once again make that data available to the victim.[13] The motive for ransomware attacks is nearly always monetary, and the demanded payment is almost always in some form of crypto-currency, typically Bitcoin.[14]

57. Various forms of ransomware have been used to attack corporate as well as individual user systems since as early as 2013. The Cryptolocker strain of ransomware posed as a Trojan horse (malware contained or incorporated within otherwise legitimate-seeming websites, applications, or attachments to emails or messages). In 2017, the WannaCry ransomware attacked and encrypted more than 300,000 Microsoft Windows systems globally, demanding payment in Bitcoin in exchange for the data decryption key. WannaCry's mode of operation closely follows ransomware's general methodology:

> When executed, the WannaCry malware first checks the "kill switch" domain name; if it is not found, then the ransomware encrypts the computer's data, then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and "laterally" to computers on the same network. As with other modern ransomware,

[13] Ransomware, http://searchsecurity.techtarget.com/definition/ransomware (last visited March 2, 2024)

[14] *Id.*

> the payload displays a message informing the user that files have been encrypted, and demands a payment of around $300 in bitcoin within three days, or $600 within seven days.[15]

58. Even where the extortionist's payment demand is relatively small (ranging between hundreds of dollars to tens of thousands of dollars), the damage wreaked on enterprise and other users' systems reaches hundreds of millions of dollars and more.

59. Unlike a data breach, whose seriousness results from the exfiltration and criminal usage of personally identifiable information, a ransomware attack renders data stored within a computer network or individual computer both unreadable and completely inaccessible to the enterprise or computer user.

60. Accordingly, banks and financial services companies, such as Evolve and Defendant Affirm, are especially attractive targets for ransomware. A Conference of State Bank Supervisors document warned that *"**[r]ansomware continues to present a major threat to the financial sector***. This method of attack used by bad actors has evolved from the basic encryption of data to now include variations utilizing double and triple extortion, as well as distributed denial of service attacks (DDoS). For the financial sector, ransomware is much more than a financial issue of paying a ransom or a fee to recover stolen data. ***Ransomware also represents an operational threat and, in some instances, a threat to the very survival of the institution***."[16]

61. Other goods and services providers are not immune from ransomware attacks. In mid-2017, pharmaceutical giant Merck was the subject of the ransomware strain known as "NotPetya." Merck's business was brought to a virtual halt, and the cost to Merck, as of October

---

[15] WannaCry Ransomware Attack, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (last visited March 2, 2024)

[16] Conference of State Bank Supervisors, "Ransomware: Lessons Learned by Banks That Suffered an Attack", https://www.dob.texas.gov/sites/default/files/files/Bank-Trust-Companies/Ransomware-Lessons-Learned-Banks.pdf (last accessed July 3, 2024), emphasis added.

2017, amounted to more than $300 million, including more than $175 million in lost business,[17] with the costs to insurers having been estimated at $275 million.[18]

62. It was widely known that ransomware attacks were a threat to banking and other financial services entities, in 2024. Indeed, the first ransomware attack was reported to occur in 1989.[19]

63. LockBit ransomware gang, which allegedly attacked Defendant Affirm and caused the Data Breach, has been very well known for many years prior to the Data Breach. According to Blackberry, "LockBit establishes control of a victim's system, collects network information, and achieves primary goals such as stealing and encrypting data. LockBit attacks typically employ a double extortion tactic to encourage victims to pay, first, to regain access to their encrypted files and then to pay again to prevent their stolen data from being posted publicly."[20]

64. LockBit gang has Russian origins. It maintains a dark web portal on The Onion Router, where it recruits talent and releases the data of victims held by companies who refuse to meet their demands.[21]

65. LockBit ransomware has been implicated in more cyberattacks this year than any other ransomware, making it the most active ransomware in the world. LockBit was first observed in September 2019.[22] It should not have come as a surprise to Defendant that LockBit ransomware

---

[17] Patrick Howell O'Neill, NotPetya Ransomware Cost Merck More than $310 Million, Cyber Scoop (Oct. 27, 2017), https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/ (last visited March 18, 2024).

[18] Reuters Staff, Merck Cyber Attack May Cost Insurers $275 Million: Verisk's PCS, Reuters (Oct. 19, 2017), https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP (last visited March 18, 2024).

[19] Nate Lord, A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, Digital Guardian (Dec. 7, 2017), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time (last visited March 18, 2024).

[20] Blackberry, "What Is LockBit Ransomware?", https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/lockbit (last accessed July 3, 2024).

[21] *Id.*

[22] *Id.*

gang would target it. Yet, Defendant failed to take basic precautions to prevent the Data Breach.

DEFENDANT FAILED TO COMPLY WITH FTC GUIDELINES

66. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

67. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[24] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

68. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[25]

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

---

[23] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 24, 2020).

[24] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited Aug. 24, 2020).

[25] FTC, *Start With Security*, *supra* note 23.

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

71. Defendant was at all times fully aware of its obligation to protect the PII of its clients because of its position as a financial services provider. Defendant was also aware of the significant repercussions that would result from its failure to do so.

PLAINTIFF AND THE CLASS SUFFERED DAMAGES

The Experiences and Injuries of Plaintiff and Class Members

72. Plaintiff and Class Members are customers of Affirm, one of the fintech apps that use Evolve as its banking partner. Plaintiff Clemmerson uses Affirm to pay for consumer products.

73. As a prerequisite of using its services, Affirm requires its customers—like Plaintiff and Class Members—to disclose their PII. It then shares that PII with Evolve, its banking partner.

74. When Affirm finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Affirm's Breach Notice fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

75. Following the Data Breach, Plaintiff Clemmerson was notified that his information was found on the dark web. Further, following the Data Breach, he also experienced a spike in spam phone calls and emails.

76. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

77. All Class Members were injured when Defendant caused their PII to be exfiltrated by cybercriminals.

78. Plaintiff and Class Members entrusted their PII to Defendant. Thus, Plaintiff and

Class Members had the reasonable expectation and understanding that Affirm would exercise reasonable care in selecting its banking services provider. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant had they known that Affirm would not take reasonable steps to safeguard their information.

79. Plaintiff and Class Members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

80. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their PII—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their PII for nefarious purposes like identity theft and fraud.

81. Plaintiff and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

82. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

83. Plaintiff and Class Members suffered injury from the misuse of their PII that can be directly traced to Defendant.

84. The ramifications of Affirm's selection of Evolve as its banking services provider, and of Evolve's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name and Social Security Number.

85. According to experts, one out of four data breach notification recipients become a

victim of identity fraud.[26]

86. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Evolve and is subject to further breaches so long as Evolve fails to undertake the appropriate measures to protect the PII in their possession.

87. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[27]

[26]Anne Saita, "Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims", Threat Post, (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited on March 18, 2024).

[27] Brian Stack, "Here's How Much Your Personal Information Is Selling for on the Dark Web," EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-

88. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

89. It can take victims years to spot or identify PII theft, giving criminals plenty of time to milk that information for cash.

90. One such example of criminals using PII for profit is the development of "Fullz" packages.[28]

91. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

92. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam

---

your-personal-information-is-selling-for-on-the-dark-web/ (last visited on March 18, 2024).

[28] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, "Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm," KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/ (last visited on March 18, 2024).

telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

93. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

94. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

95. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

96. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

97. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

98. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[29]

[29] "Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable," FED. TRADE COMMISSION (Dec. 7, 2009),

99. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[30] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[31]

100. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[32] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTCA.

101. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. See *In the matter of Lookout Services, Inc.*, No. C-4326, Complaint ⁋ 7 (June 15, 2011) ("[Respondent] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Respondent] failed to employ sufficient measures to detect unauthorized access."); *In the matter*

---

https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on March 18, 2024).

[30] "Start With Security, A Guide for Business," FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 18, 2024).

[31] *Id.*

[32] "Taking Charge, What to Do If Your Identity is Stolen," U.S. DEPARTMENT OF JUSTICE, at 3 (January 2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited on March 18, 2024).

of The TJX Cos., Inc., No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Respondent] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . .").

102. These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII.

103. Charged with handling highly sensitive PII including, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the PII that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's customers as a result of a breach. Affirm nevertheless failed to inquire which, if any, security measures Evolve employed to safeguard its clients' information before selecting Evolve as its data storage services provider.

104. Affirm's selection of Evolve as its data storage services provider and Affirm's failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

105. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

106. Plaintiff seeks relief in his individual capacity and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of the following subclasses (together, the "Class"):

> All customers of Affirm Inc., located in the United States, whose PII was affected by the data breach which occurred at Evolve on or about June 25, 2024.

107. Excluded from the above Class are Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

108. **Numerosity**. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, Defendant provides services to hundreds of thousands of individual clients.

109. **Commonality**. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. If Affirm failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their PII;

f. If Defendant breached their duty to Class Members to safeguard their PII;

g. If Defendant knew or should have known that Defendant's data security systems and monitoring processes were deficient;

h. If Defendant should have discovered the Data Breach earlier;

i. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If Defendant's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. If Defendant's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If Defendant's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

o. If Affirm breached its contracts with Plaintiff and Class Members;

p. If Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

q. If Defendant failed to provide notice of the Data Breach in a timely manner; and

r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

110. All members of the proposed Class are readily ascertainable. Defendant has access to the addresses and other contact information for members of the Class, which can be used for providing notice to many Class members.

111. **Typicality**. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like every other Class Member's, was impacted by the Data Breach.

112. **Adequacy of Representation**. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and

adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

113. **Superiority of Class Action**. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

114. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

115. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

116. Plaintiff re-alleges and incorporates by reference paragraphs 1-115 of the Complaint as if fully set forth herein.

117. Defendant Affirm required its customers, including Plaintiff and Class Members, to submit their non-public PII to Defendant to receive Defendant's services.

118. Affirm owed a duty to Plaintiff and Class Members to select a data storage services provider that employed reasonable data security measures to protect their PII and other information. Affirm failed to conduct a reasonable, or any, inquiry when it selected Evolve to provide banking services and store its clients' sensitive information.

119. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable to Defendant. Given that Evolve—jthe third-party bank to whom Affirm entrusted Plaintiff's and Class Member's information—holds vast amounts of PII, it was inevitable that unauthorized individuals would at some point try to access Evolve's databases of PII.

120. After all, PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to Defendant.

121. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their, or their service providers', systems and networks, and the personnel responsible for them, adequately protected the PII.

122. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that its, and its service providers', systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

123. Defendant failed to take appropriate measures to protect the PII of Plaintiff and the Class. Defendant is morally culpable, given the prominence of security breaches in the financial services industry, including the insurance industry. Any purported safeguards that Defendant had in place were wholly inadequate.

124. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the financial service industry, and allowing unauthorized access to Plaintiff's and the other Class Members' PII. In addition, Affirm breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to conduct adequate due diligence on Evolve's data security practices and procedures before engaging Evolve as its banking services provider.

125. The Defendant was negligent in failing to comply with industry and federal regulations in respect of safeguarding and protecting Plaintiff's and Class Members' PII.

126. But for Defendant's wrongful and negligent breach of their duties to Plaintiff and the

Classes, Plaintiff's and Class Members' PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Classes and all resulting damages.

127. Defendant owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

128. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the PII of Plaintiff and Class Members.

129. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. In addition, Affirm breached its duties by failing to conduct an adequate inquiry into Evolve's data security practices and procedures, before engaging Evolve as its banking services provider. But for Defendant's negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to comply with—and thus violating—FTCA and its regulations;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to conduct an adequate inquiry into Evolve's data security practices and procedures;

e. Failing to have in place mitigation policies and procedures;

f. Allowing unauthorized access to Class Members' PII;

g. Failing to detect in a timely manner that Class Members' PII had been

compromised; and

h. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

130. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial service industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

131. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. Defendant knew or should have known that its systems and technologies for processing and securing the PII of Plaintiff and the Classes had security vulnerabilities.

132. As a result of Defendant's negligence, the PII and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of identity theft and their PII being disclosed to third parties without the consent of Plaintiff and the Class members.

133. Simply put, Defendant's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

134. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

135. Plaintiff re-alleges and incorporates by reference paragraphs 1-115 of the Complaint

as if fully set forth herein.

136. Under the FTCA, Defendant had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.[33]

137. Moreover, Plaintiff's and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiff and Class Members.

138. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

139. Defendant's failure to comply with FTCA statutory duties and standards of conduct constitutes negligence *per se*. Defendant's failure to comply with the requisite standard of care caused the Breach, exposing Plaintiff's and Class Members' PII to cyber-criminal and causing Plaintiff and Class Members pecuniary and non-pecuniary harm detailed herein.

140. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (1) strengthen its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for the remainders of their lives.

THIRD CAUSE OF ACTION
Breach of Contract
(On Behalf of the Plaintiff and the Class)

141. Plaintiff re-alleges and incorporates by reference paragraphs 1-115 of the Complaint as if fully set forth herein.

142. Plaintiff and Class Members entered into valid and enforceable contracts through

[33] 15 U.S.C. § 45.

which they provided labor and their PII to Defendant. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' PII.

143. Plaintiff and Class Members fully performed their obligations under their contracts with Defendant.

144. However, Defendant did not secure, safeguard, and/or keep private Plaintiff's and Class Members' PII, and therefore Defendant breached its contracts with Plaintiff and Class Members.

145. Defendant allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' PII without permission. Therefore, Defendant breached the contract with Plaintiff and Class Members.

146. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiff and Class Members.

147. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

148. Plaintiff and Class Members are entitled to compensatory, consequential and nominal damages suffered as a result of the Data Breach.

149. Plaintiff and Class Members would not have entered into employment contract with Defendant, or would have demanded significantly higher wages, had they been aware that Defendant would fail to take basic precautions to safeguard their PII.

150. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Class Members for a period of ten years.

FOURTH CAUSE OF ACTION
Implied Contract
(On Behalf of the Plaintiff and the Class)

151. Plaintiff re-alleges and incorporates by reference paragraphs 1-115 of the Complaint as if fully set forth herein.

152. This cause of action is pleaded in the alternative to breach of contract, above.

153. Plaintiff and Class Members were required to deliver their PII to Evolve as part of using apps provided by Defendant, because Evolve was Defendant's banking partner.

154. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant, who provided it to Evolve.

155. Defendant accepted possession of Plaintiff's and Class Members' PII, for the ostensible purpose of providing financial services to them, as users of Affirm app.

156. Plaintiff and Class Members entrusted their PII to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

157. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

158. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

159. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

160. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

161. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

162. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant. Defendant, on the other hand, breached its obligations under the implied contracts with Plaintiff and Class Members by failing to safeguard their PII and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

163. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) theft of their PII; (ii) lost or diminished value of PII; (iii) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

164. Plaintiff and Class Members are entitled to compensatory, consequential and nominal damages suffered as a result of the Data Breach.

165. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members for a lifetime.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

166. Plaintiff re-alleges and incorporates by reference paragraphs 1-115 of the Complaint as if fully set forth herein.

167. This cause of action is plead in the alternative to the breach of contract and breach of implied contract theory.

168. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying money for Affirm's services, a portion of which was passed on by Affirm to Evolve, and was intended to have been used by Defendant for data security measures to secure Plaintiff and Class Members' PII. Plaintiff and Class Members further conferred a benefit on Defendant in the form of their PII from which Defendant derived profits.

169. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Affirm's failure to provide adequate security.

170. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

171. Defendant acquired the monetary benefit, PII, through inequitable means in that Defendant failed to disclose their inadequate security practices, previously alleged, and failed to maintain adequate data security.

172. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to give their money—or disclosed their data—to Affirm.

173. Plaintiff and Class Members have no adequate remedy at law.

174. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII is used; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (5) lost

opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach.

175. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

176. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative, and the undersigned as Class Counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the

privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xi. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor

Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. An injunction enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: August 28, 2024

MORGAN AND MORGAN
COMPLEX LITIGATION GROUP

By: /s/ Michael F. Ram

Michael F. Ram (SBN 104805)

mram@forthepeople.com
MORGAN AND MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Ave, Suite 500
San Francisco, CA 94102
T: (415) 846-3862
F: (415) 358-6923

John A. Yanchunis*
JYanchunis@forthepeople.com
Ronald Podolny*
ronald.podolny@forthepeople.com
Antonio Arzola*
ararzola@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

**Pro hac vice forthcoming*

Counsel for Plaintiff and the Proposed Class